

REMARKS/ARGUMENTS

The Examiner is thanked for his continuing attention to this application.

However, as to the rejected claims, Applicant respectfully traverses the rejections. The bases for this traversal are discussed below.

35 U.S.C. §101

Claims 3-19 and 33 are rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter. Applicant traverses. The fact that the program is transmissible, as indicated by the specification, **does not negate that it is stored on a computer readable medium**. In general, computer logic routines are encoded in digital data format and stored in some tangible medium, such as solid state memory (RAM or ROM) or other media (such as disk drives). Whether or not the file **is in addition transmissible**, should not render the claim non-statutory.

The paragraph to which the examiner refers, states, in full:

[0196] The invention may be embodied in a fixed media or transmissible program component containing logic instructions and/or data that when loaded into an appropriately configured computing device cause that device to perform in accordance with the invention.

Applicant does not understand the basis of the examiner's objection. In order to expedite prosecution, Applicant has added the limitation "fixed" to the rejected claims. As applicant has argued previously, all logic executed by a computer system is at some point stored in a fixed media, whether that media be RAM or ROM memory (such as in a running computer), persistent RAM memory (such as in a USB-drive), or electronically or optically recorded media (such as a magnetic hard disk or floppy disk, a CD, or a harddisk). If the Examiner maintains his rejection on this issue, Applicant hereby requests a telephone interview regarding this matter.

35 U.S.C. §102(e)

Claims 1-13 and 15-33 stand rejected under 35 U.S.C. § 102(e) under Sorkin. Applicant makes the following observations regarding Sorkin while reserving Applicant's rights to contest the prior invention conclusion.

As a basis for his rejections, of claim 1, the examiner cites (Col. 14, Line 37 to Col. 16, Line 4). The last paragraph therein reads:

In one embodiment, at least one of the steps of the process illustrated in FIG. 10 is implemented by replacing one or more operating system functions in the system entry (or "sysent") table with a new program designed to perform the above-described filtering function. In one embodiment, the new program returns the output of the original operating system function if access to a requested file (or process) is permitted (i.e., the file or process is within the virtual cage) and returns an indication that the file (or process) does not exist, if the file (or process) is not inside the cage. In one embodiment, a similar approach is used to modify the function that responds to system calls such as "kill", in order to permit intruders to terminate only processes running inside the cage.

While this passage suggests some similarities between some of the techniques of Sorkin and the claimed invention, Sorkin does not teach at the operating system level and on a request basis providing deceptions. Sorkin, as indicated throughout, suggests that security is provided by identifying specific users as intruders and assigning them to "cages" with a generated "content set" responses or actions at the operating system. See, for example, the summary:

Content sets are generated for a computer associated with the network. It is determined whether a user should be routed to the generated content sets. If it is determined that the user should be routed to the generated content sets, a generated content set is selected and the user is so routed. Various actions and events may be recorded in a logfile, and the logfile is analyzed using regular expressions.

As well as claim 1.

1. A method for providing security for a computer network, comprising: generating content sets for a computer associated with the network; determining whether a user should be routed to the generated content sets; selecting one of the content sets if it is determined that the user should be routed to the generated content sets; routing the user to a network interface associated with the selected generated content set; monitoring the activities of the user with respect to the computer; preventing the user from accessing files associated with said monitoring; and preventing the user from accessing processes associated with said monitoring; wherein each generated content set is associated with one or more network interfaces associated only with that generated content set.

The present invention teaches a more flexible and general approach wherein deceptions can be provided as a response to any system request and are provided without the

need of assigning particular users to "cages." Sorkin teaches away from the claimed invention in that it describes "cages" and "content sets" as being necessary for providing network security.

Fundamentally, Sorkin deals with separation of content sets. The means used to do this is the use of virtual machines (VMs) within a computer. The present invention alters the operation of a computer so as to allow a far broader set of responses and to do so in a way that allows finer granularity of discrimination. For example, the invention can allow legitimate operations to be executed while only doing deceptions on specific illegitimate activities. Sorkin, in contrast, forces the user into a VM for all activities. Sorkin is not modifying the operating system operation; but is instead making completely independent operating systems for each VM.

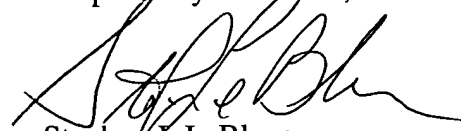
Access controls - which is what Sorkin is teaching with regard to the kill function and restricted access to files - has been in existence for a long time. Starting with the trusted systems of the 1970s files not authorized to be accessed by users have not been shown as present, and processes not authorized for the user have been prevented from appearing in the users' process list and cannot be killed. It is only access control, and not deception that Sorkin teaches.

Sorkin furthermore uses syntax as the approach to detection and response. An operating system (OS) approach as described in the present invention is far better in that all syntax methods such as Sorkin can be readily fooled whereas OS-level replacements do not suffer from this handicap.

If after consideration of the above response, the Examiner does not find that all pending claims are in condition for allowance, **applicant hereby requests a telephone interview with the Examiner. Please contact the undersigned at (510) 769-3508.**

QUINE INTELLECTUAL PROPERTY LAW GROUP
P.O. BOX 458, Alameda, CA 94501
Tel: 510 337-7871
Fax: 510 337-7877
PTO Customer No.: 22798
Deposit Account No.: 50-0893

Respectfully submitted,



Stephen J. LeBlanc
Reg. No: 36,579